

(19) World Intellectual Property  
Organization  
International Bureau



08 JUL 2004

(43) International Publication Date  
11 November 2004 (11.11.2004)

PCT

(10) International Publication Number  
WO 2004/097602 A2

(51) International Patent Classification<sup>7</sup>: G06F 1/00

[GB/GB]; Star Internet, Brighthouse Court, Barmwood,  
Gloucester GL4 3RT (GB).

(21) International Application Number:

PCT/GB2004/001333

(74) Agents: AYERS, Martyn et al.; J.A. Kemp & Co., 14  
South Square, Gray's Inn, London WC1R 5JJ (GB).

(22) International Filing Date: 29 March 2004 (29.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
0309463.8 25 April 2003 (25.04.2003) GB

(71) Applicant (for all designated States except US): MES-  
SAGELABS LIMITED [GB/GB]; 1270 Lansdowne  
Court, Gloucester Business Park, Gloucester LG3 4AB  
(GB).

(81) Designated States (unless otherwise indicated, for every  
kind of national protection available): AE, AG, AI., AM,  
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,  
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,  
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,  
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,  
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,  
PH, PI., PT, RO, RU, SC, SD, SE, SG, SK, SI., SY, TJ, TM,  
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,  
ZW.

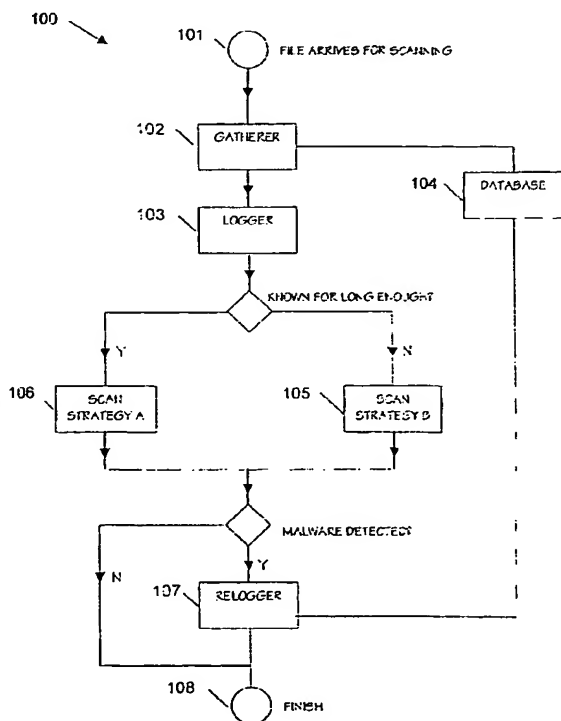
(72) Inventor; and

(75) Inventor/Applicant (for US only): SHIPP, Alexander

(84) Designated States (unless otherwise indicated, for every  
kind of regional protection available): ARIPO (BW, GH,  
GM, KE, LS, MW, MZ, SD, SI., SZ, TZ, UG, ZM, ZW).

[Continued on next page]

(54) Title: A METHOD OF, AND SYSTEM FOR, HEURISTICALLY DETERMINING THAT AN UNKNOWN FILE IS HARM-  
LESS BY USING TRAFFIC HEURISTICS



(57) Abstract: A system for processing a computer file to determine whether it contains a virus or other malware maintains a database of known files which it references to determine whether the file is an instance of a known file, and if so, whether it has been known about long enough that it can be regarded as safe. If it can be regarded as safe, the file is subject to less thorough processing for detecting malware, or no such processing at all.

WO 2004/097602 A2